HTTP://www.dotnetrocks.com

Carl Franklin and Richard Campbell interview experts to bring you insights into .NET technology and the state of software development. More than just a dry interview show, we have fun! Original Music! Prizes! Check out what you've been missing!

Text Transcript of Show #593
(Transcription services provided by PWOP Productions)

Pat Hynds Still Cares About Security
September 14, 2010

Our Sponsor

HTTP://www.telerik.com/

Geoff Maciolek: The opinions and viewpoints expressed in .NET Rocks! are not necessarily those of its sponsors, or of Microsoft Corporation, its partners, or employees. .NET Rocks! is a production of Franklins.NET, which is solely responsible for its content. Franklins.NET - Training Developers to Work Smarter.

[Music]

Lawrence Ryan: Hey, Rock heads! Disassemble your Lego Mindstorm air conditioner and listen up! It's time for another stellar episode of .NET Rocks! the Internet audio talk show for .NET developers, with Carl Franklin and Richard Campbell. This is Lawrence Ryan announcing show #593, with guest Pat Hynds, recorded live Saturday, June 26, 2010. .NET Rocks! is brought to you by Franklins.NET - Training Developers to Work Smarter and now offering Silverlight 4.0 video training with Billy Hollis on DVD, dnrTV style, order your copy now at www.franklins.net. Support is also provided by Telerik, combining the best in Windows Forms and ASP.NET controls with first class customer service, online at www.telerik.com, and by Haystack Code Generator for .NET: Code Generation on Steroids! Online at codehaystack.com. And now, the man who while hunting saw a sign that said "bear left" so he went home, Carl Franklin.

Carl Franklin: Hey, I'm here. We're here.

Richard Campbell: Nice of you to come by.

Carl Franklin: I'm sorry. You know, I realized I didn't have a cup of coffee and then I had made a pot of coffee but it's been so long since I made a pot with my Cuisinart, you know, sort of all-in-one grinder brewer that I think some coffee grounds got lodged in the filter thing or something and so what I ended up with was a pot of lightly brown-toned hot water.

Richard Campbell: Nice.

Pat Hynds: Really?

Carl Franklin: Yeah. So I had to run out.

Pat Hynds: I figured you guys would be mainlining coffee this whole weekend.

Carl Franklin: Yeah, we are. We'll fix that some other time.

Richard Campbell: Yeah.

Carl Franklin: But I do have a one-off coffee cup maker so like a Keurig machine.

Pat Hynds: Ah, okay.

Carl Franklin: So there you go. Well, I got to announce first of all thank you for listening if you're up this early, I can't believe you must be, but...

Pat Hynds: So Pat, what are you working on these days?

Carl Franklin: Yeah.

Pat Hynds: Well, there are actually two major things. One is the Locked Down podcast, which we're hoping to start broadcasting soon with Michele Leroux Bustamante.

Richard Campbell: You got a few shows in the can now.

Carl Franklin: And it's a security oriented podcast, right?

Pat Hynds: Very much so, yeah. Carl's helping me conquer the microphone beast so I had to order new equipment and apparently...

Carl Franklin: And it's a big bad beast too, let me tell you.

Pat Hynds: Oh, my. Well, yesterday I don't know what was going on but I just ordered new equipment so hopefully that will be out. I'm very excited about that. Michele has a new security business that she's working on as well.

Richard Campbell: Right.

Pat Hynds: All my endeavors focus around the security so we're kind of excited to be talking of all the luminaries, Keith Brown, Paula Yankovic?

Richard Campbell: Januszkiewicz.

Pat Hynds: Januszkiewicz.

Richard Campbell: You were close.

Carl Franklin: No, no, wait. It's a different Paula but she's also from Poland. It's not Paula Januszkiewicz.

Richard Campbell: Yeah, it is.

Carl Franklin: It is?

Richard Campbell: Yeah.

Pat Hynds: Yeah, it is.

Carl Franklin: Okay, I'm sorry.

Richard Campbell: And that's the same girl who entered Speaker Idol a couple of times and...

Carl Franklin: No, that's not her.

Richard Campbell: That's her.

Pat Hynds: It is her.

Carl Franklin: All right. So we were mistaken.

Richard Campbell: No, that is her.

Carl Franklin: When I talked to Pat, I thought he didn't know that she did Speaker Idol so we thought it was somebody else.

Richard Campbell: Same girl.

Pat Hynds: Oh, no I did.

Richard Campbell: It's hard to imagine but it is really the same girl.

Pat Hynds: Yup.

Carl Franklin: All right. Cool.

Pat Hynds: And the first guest is Carl.

Carl Franklin: Yeah, of course.

Richard Campbell: Are you really?

Pat Hynds: Yeah.

Carl Franklin: Because I know so much about security.

Richard Campbell: You're a very secure person, that much I know, yeah.

Carl Franklin: I am very secure.

Pat Hynds: We figured we would start with the person who knows everything about everything in the .NET world because he's talked to everybody about everything in the .NET world and see how much people don't know about security.

Carl Franklin: Well, I am a generalist and I know one thing, that developers hate security.

Pat Hynds: Yeah and so we actually set the tone quite well. So that's one major effort, and then the other is I'm trying to push a product out the door. As you may know I left CriticalSites on very good terms. They're still doing well, and I pursued an old company that I've been running in the background thread for a long time called DTS. If you've seen any of the How Do I videos, a good chunk of the How Do I videos they're on Silverlight.NET, ASP.NET, even on MSDN.

Carl Franklin: What are the How Do I videos?

Pat Hynds: They're small chunks of data, a presenter, an MVP, RD, or somebody who's involved in the community who works with us and creates a video that shows how to do something and Microsoft is directing the project with us and we create these videos for the community sites and for Microsoft's main properties. Very high standards about how they're going to work and what they're going to show, etc. I think we've done 1,500 of them so far for Microsoft.

Richard Campbell: Wow. Are you kidding me?

Pat Hynds: No.

Richard Campbell: And they're quick too, right? They're 5, 10 minutes?

Pat Hynds: They're 8 to 15 most of the time. We have some that are 35, 40 minutes because you can't get some things done unless you're -- we're tackling very hard topics in some cases.

Richard Campbell: Right.

Pat Hynds: So some of them do get a little long in the tooth, but they're quite useful. I even use them for my stuff. So DTS is the producer of those. It does security audit. It does a lot of things that CriticalSites used to do, and then we're actually a product company as well. We've been working on a product since last summer that's going to solve the problem of security ownership in large file systems. One of the things that I noticed in my travels, because I do a lot of stuff with data security as well as general coding security, is that ownership of files is one of those dirty little secrets on most networks. Most of the time, the data on a 50 terabyte network has been migrated one or more times.

Richard Campbell: Right.

Pat Hynds: Most of the time in those migrations, the administrator ends up owning everything or a user who longer works for the company or who longer works in the department owns all the most important files.

Carl Franklin: Yeah, right.

Pat Hynds: And ownership is one of those things that everybody ignores because it's hard. It hard to go through and set ownership correctly because the tools just aren't there. So we've built a

rules-based utility that has really interesting capabilities such as I can say I want everyone to own their home directory and everything in it and it will go through, you pick which drives you want to apply to and it will go in and look in Active Directory, figure out what their home directory is and make sure that user owns everything in it. That makes things like code to software, charge back software, and all the other storage management products that have been coming out over the last 5, 10 years work much better.

Carl Franklin: By the way, Malcolm Smith from Australia says "Hi, guys. We hear you here in Australia loud and clear. It's 10:00 p.m. Nice music, Carl. Also can we buy a CD of your band?" Not yet. You will be able to, but it's good to know that Australia is listening.

Pat Hynds: That is awesome.

Carl Franklin: Go ahead.

Pat Hynds: No, no, no. That's it. So that's the first product. And the second product, what we probably are going to be doing is we had to build a licensing system for that product and so we looked around at the various licensing systems that ISVs were able to buy and we weren't really thrilled with the offerings so we built our own and we are considering making that a public offering as well.

Carl Franklin: This is not the first security tool that you've built. I mean, you did a lot of work at CriticalSites building security tools, right?

Pat Hynds: Yeah. At CriticalSites and NTP Software, the sister company for CriticalSites owned by my really good friend of NTP Software, Bruce Backa, they are a product company 100%, and NTP Software and CriticalSites are kind of sister companies. Bruce has always run a consulting company with a software company so that the weaknesses of each actually turn into strengths for each other. It's a very interesting model and I'm trying to follow on those footsteps by having the consulting side of DTS work with the software side of DTS to cancel out the weaknesses.

Carl Franklin: Can we talk about any of those products?

Pat Hynds: Yeah, certainly we could. Yeah.

Carl Franklin: I remember the one that you were working on like in .NET 1.0 or something.

Pat Hynds: Oh, yeah. Yeah.

Carl Franklin: It was about storage or something like that.

Pat Hynds: That's where my storage management background comes from.

Carl Franklin: Storage Reporter?

Pat Hynds: So that was an original attempt, yes, and then that was sold off to another company and they've since gone into other reporting systems that are based on .NET. So right now, what NTP is building or working on is they're taking their Storage Management reporting product called storage modeling and analysis and they're redoing it to be called File Reporter. I really, really hope I'm not outing things that I shouldn't before they're announced, but I'm really excited about it because it takes all the goodness of Storage M&A and we've implemented that for some of the largest banks and largest industrial manufacturers in the world and I still work with NTP Software pretty regularly consulting for large companies.

Carl Franklin: What's Storage M&A?

Pat Hynds: Modeling and Analysis.

Carl Franklin: Oh, M&A.

Pat Hynds: Basically you've got 100 terabytes of storage and you want to know what are people doing with it and should I be going and hitting them with 2 x 4's because of it.

Richard Campbell: Well, how many times, even in your own machine you've seen I'm down to a gig, what's eating up my 500 gigs disk space like where is everything?

Pat Hynds: Exactly.

Carl Franklin: Or even just can you tell me when disk space is low because that's like a little alarm that you never, ever get. You know what I mean? Until it crashes.

Richard Campbell: Yeah.

Carl Franklin: You're into this lately, didn't you?

Richard Campbell: While we're on the road trip.

Carl Franklin: While we're on the road trip.

Richard Campbell: While we're on the road trip, my Exchange -- you know I'm crazy, I run my own Exchange Server in my Server closet at home. So start with you have a Server closet at home.

Carl Franklin: Don't do that.

Richard Campbell: Yeah. You can stop that, that's not right.

Carl Franklin: You could have a Cloud.

Richard Campbell: I could have, yeah. You know, it's a good experience to exercise using these tools. You know, I still come to the realization that the only piece of software from Microsoft that I truly fear is Exchange. What happened with Exchange is mail just stop coming into my inbox, coming into all the inboxes of the Exchange Server I own.

Carl Franklin: Right. That's the symptom.

Richard Campbell: No errors, no crashes, the server is running, I could get to it. I can send mail, no problem. No mails coming in, and I finally RDP into those servers to look around and there in the event log is "You're low in disk space, we won't be delivering anymore mail now."

Pat Hynds: Yeah. I speak for that exact reason. I'm actually sitting next to my rack with my Exchange Server in it and I'm in the process of upgrading my drives to 2 terabytes SATA drive.

Richard Campbell: Nice.

Pat Hynds: Even though they're slower because the system came with 15K drive, but I just need that much more space. Right now I've got 400 gigs free and soon I'm going to have 3.8 gigs terabytes free.

Richard Campbell: Because somehow you'll get by with that thing.

Pat Hynds: I think so.

Richard Campbell: I just love the fact that two of us on this show right now run our own Exchange Servers.

Carl Franklin: Yeah, I know better. You know, I never did that and there's good reason for it because everyone I know who runs Exchange has slightly less hair than I do.

Pat Hynds: I'm actually looking to get an alternate site. I may be putting a rack at my nephew's house, because he works at DTS, so that we can do some of the more advanced high availability stuff.

Richard Campbell: Right. Distribute over to that one as well.

Pat Hynds: Yeah. The problem with that is you need another computer to form the quorum.

Richard Campbell: Right.

Pat Hynds: And so I'm wondering do I create a third site because it's site-to-site.

Richard Campbell: Right.

Pat Hynds: Do I create a third site or do I just put a witness as a VM in each of the systems?

Richard Campbell: Yeah. I like the mutual witness approach just because that way there's no single point.

Pat Hynds: Well, but you could then get -- the thing is what if the network link goes down and both sites think they're the only one alive?

Richard Campbell: Right. And then all hell breaks loose.

Pat Hynds: Right. So that's the one scenario I'm still trying to fight with.

Richard Campbell: You know, for me, running out of disk space... So we're in Atlanta so I had to do this all remotely. I'm running my Exchange Server as virtual machine so literally I was able to go into SCVMM and say give that virtual machine another 20 gigs of disk space and it went okay and then starts working again.

Carl Franklin: Yeah.

Pat Hynds: Oh, cool. Yeah, I love virtualization.

Richard Campbell: Well, the fact that Exchange didn't drop any mail, it was just holding the mail in the queue, it's just pushing it out to the individual boxes, it needs a lot more disk space, and then holding it in the input queue.

Pat Hynds: Well, I use a mailbag. I have a hosted server at one of the hosting facilities and we just have a mailbag. So it goes in there, and if I have to reboot the server I don't miss any mail.

Richard Campbell: Right.

Pat Hynds: So this is turning into a RunAs show, hasn't it?

Richard Campbell: Yeah. It really has.

Pat Hynds: So back to what you were asking, so NTP Storage M&A and soon to be File

Reporter product is actually quite full because right now it reports on Exchange is and on the file system. It's not for users, for their desktops. It's for the enterprise.

Richard Campbell: Right.

Pat Hynds: And they're adding features like, or at least on the road map there are features like SharePoint and some really, really cool stuff. They've really gotten the whole design paradigm of getting the information quickly. I've actually got to see a pre-release version of the software just because I'm in the developer's area all the time and it's looking very slick. So that's where I cut my teeth on product management.

Carl Franklin: Yeah.

Pat Hynds: On, you know, commercial product management.

Carl Franklin: Pat, what was some of the -- I mean, you did a lot of security work where you went into companies and did an analysis to find out where their vulnerable points are and try to beef them up a little bit.

Pat Hynds: Yeah.

Carl Franklin: Do you have any, and I know this is, you know, you don't want to give names or anything, but are there any really truly scary stories?

Pat Hynds: So it depends on what spectrum. Yes, there are.

Carl Franklin: How many? Can you share?

Pat Hynds: I do. I'll just protect the names of the guilty.

Carl Franklin: Right.

Pat Hynds: So it depends on what level of the spectrum you want to be on because there are both extremes. There's the major, major company that I went to back in the early days of SQL back when SQL 6.5 was new and they said, the administrator that I've talked to, the database administrator called because they were really thinking about getting rid of Microsoft SQL Server and going back to Ingress, or Informix, or whatever they run before that and the reason was because they said the system was unstable, it wasn't reliable. You know, it was losing data.

Carl Franklin: What?

Pat Hynds: Yeah. I know, I know, I know. SQL doesn't lose data.

Carl Franklin: Yeah.

Pat Hynds: And I've been teaching SQL back for two days. I taught Microsoft SQL Server at Sybase back for two days. So I've been around the block for a while. I went in and the administrator I talked to was very nice and had a lot of experience with the old database system and no training whatsoever on Microsoft SQL Server.

Richard Campbell: Right.

Pat Hynds: The first thing that struck me is this has been the Achilles heel for Microsoft SQL Server since then and is today which is no one ever lets anyone touch an Oracle server unless they've got a certificate.

Richard Campbell: Right.

Pat Hynds: Unless they've gone to training, they've been read the right act, you have to apprentice typically before you get to actually touch the production Oracle server. But the temp gets to, you know, be the administrator of the SQL Server because they've made the interfaces so easy.

Richard Campbell: Yeah. There's another side to this which is if you don't know exactly what you're doing, you get nowhere with Oracle. You can't even get started.

Pat Hynds: Right.

Richard Campbell: It's just impenetrable and you can fake your way through enough SQL Server to get something that seems like a database even though none of the things that are important to a database, like reliability and so forth, are working.

Pat Hynds: Yeah and that's exactly...

Carl Franklin: Details.

Pat Hynds: Well, it's been a great strength for Microsoft because it has opened it up to people who would never have touched databases, but it's also Microsoft gets blamed for all of these horror stories so hopefully we'll shed some light on this one. So you'll love this. The company was full of scientists, 400 technical users who weren't techies but had advance degrees, management degrees.

Carl Franklin: Scientists, what do they know?

Pat Hynds: Exactly. Well, they know how to do a little SQL that drops tables.

Richard Campbell: Right.

Pat Hynds: And it turned out that when I started talking about security models, this administrator said "Well, yeah. We have a security model. Everybody has to log in to get to the system." I said, "Oh, okay. Good. How are you doing that? Are you doing that through Windows? Are they logging in?" He says, "SA."

Richard Campbell: Nice. They all have to log in with SA.

Pat Hynds: They all log in. They have 400 users logging with SA and they're wondering why some data was missing.

Richard Campbell: Right.

Carl Franklin: Oh, that's too bad.

Pat Hynds: Well, because some people were learning how to delete things. So that was one and we save that SQL Server state there, they're database, and actually they're very big customer of Microsoft now and at that time they were just trying it out. This was when Microsoft was just starting to get straight CRUD in the enterprise.

Carl Franklin: Yeah.

Pat Hynds: So that was actually a fun one. Then there's the other side of the extreme. There was a company we've dealt with that I really enjoyed dealing with, and I'd probably going to call them back now, who we did security on pretty regularly and they were so rabidly security conscious. I haven't seen that since I was visiting the marines in Quantico.

Richard Campbell: Nice.

Carl Franklin: Wow.

Pat Hynds: Their information on their network was the business. If someone broke into the database, if someone got their information, they were out of business.

Richard Campbell: Right.

Pat Hynds: It wasn't a question. Just the fact that someone got in made them out of business and so they took it very seriously. They did not allow people at their desktop to have internet access.

Carl Franklin: Wow.

Richard Campbell: That's pretty rabid.

Pat Hynds: Everyone had to forward emails going outside the organization to the security guy.

Carl Franklin: Wow.

Pat Hynds: He would then send them outside the organization. Yeah, they were really...

Richard Campbell: A live firewall.

Pat Hynds: Yes, yes.

Carl Franklin: Yeah, that's right.

Pat Hynds: He's a really good guy actually. But what I meant is people only send emails outside of the organization if they really, really needed to.

Richard Campbell: Yeah.

Pat Hynds: And there was no, you know, hey, how do you like them Mets, or anything like that going on.

Carl Franklin: At least they don't have the problem with employees surfing porn while they should be working.

Pat Hynds: Exactly, yeah. That just didn't happen.

Carl Franklin: Or distraction in general. I mean, that's really what I mean.

Pat Hynds: They were the first company I ever talked to that actually uses Superglue in their USB ports.

Richard Campbell: To block them. Yeah, fill them with epoxy.

Carl Franklin: Richard is nodding like he's heard of this.

Richard Campbell: Oh, no. I have epoxied USB ports.

Carl Franklin: You have.

Richard Campbell: I've also pulled floppy drives out of machines. I've stripped machines so that there's no physical way to remove data from the machine.

Carl Franklin: Wow. What a great idea. I mean, I'm always all about the low tech solutions first like lock your machine, yeah, put it in a room with a lock.

Richard Campbell: Because it's only in the latest versions of Windows that they've actually gotten a workable solution for you can't transfer stuff onto a USB key and take it outside without anybody knowing.

Carl Franklin: So tell me about that. What is that?

Richard Campbell: How do you do that today?

Carl Franklin: Yeah, yeah.

Richard Campbell: There are new group policy rules inside of Windows 2008 and Windows 7.0 where basically anytime you a USB key is plugged in and out of a machine, it writes a record of so we have a clear audit trail of you plug a USB key in there and so on.

Carl Franklin: What about if you just press F8 while you're booting up and go to a command prompt and go to your hard drive and start copying files?

Richard Campbell: Yeah, you could lock all that down too, and actually these days NTFS is pretty good about you can't boot a drive from another machine and get access to the files.

Carl Franklin: I actually should listen to RunAs Radio more often I think.

Pat Hynds: Although the Achilles heel of every security mechanism is physical possession.

Richard Campbell: Yeah.

Pat Hynds: If a hacker physically possesses the machine, you could build as many impediments as you want or even BitLocker.

Richard Campbell: It's just time.

Pat Hynds: It's just time, yeah. With BitLocker I think that's probably the big gun.

Richard Campbell: Yeah. If BitLocker is done right now, you're in the I will crack this. It may take a quadrillion years, but I will crack this.

Carl Franklin: BitLocker is one of those tools that shipped in Vista and everybody was so busy throwing rocks to Vista that I never even really understood what it was.

Richard Campbell: It's really only -- but it's only in the enterprise and ultimate edition.

Carl Franklin: Yeah. Is BitLocker essentially just a way to say this...?

Pat Hynds: Encrypting hard drives.

Carl Franklin: I thought it is a good way to say maybe this is just one of the things that it does saying this folder right here I want only me to be able to access it.

Richard Campbell: NTFS does that.

Pat Hynds: Yeah. It's more of a "my disk is encrypted." If you don't actually know the right way to access this, you can't see anything. My disk is a pile of goo if you don't know the secret sauce.

Carl Franklin: But isn't the secret sauce just being able to log in?

Pat Hynds: Yeah, it is.

Carl Franklin: How much more does it have than NTFS?

Richard Campbell: With NTFS, I could still see the directory but I would get an access denied if I try to look at the directory.

Carl Franklin: Well, that's if you're logged as someone else.

Pat Hynds: So without BitLocker, I can boot to an ultimate operating system and I can see the whole drive.

Richard Campbell: Right.

Pat Hynds: With BitLocker, I boot off an operating system and I see an unformatted -- well, I think it still shows that it's formatted, but I see a drive with randomness that I can't interpret.

Carl Franklin: And it doesn't interpret it as a disk carrier and say do you want to format this drive because it's messed up.

Pat Hynds: I don't think so.

Richard Campbell: Actually it will.

Carl Franklin: Really?

Richard Campbell: Yeah. It says "I don't understand this format. Do you want to reformat?"

Carl Franklin: Whoa.

Richard Campbell: Yeah.

Pat Hynds: Oh, I didn't realize that. Oh, that's interesting.

Carl Franklin: That's not very smart.

Richard Campbell: Well, that's pretty effective actually. It keeps your data protected.

Carl Franklin: Unless somebody reformats it by mistake.

Richard Campbell: No.

Pat Hynds: I'd rather they format it and steal it.

Richard Campbell: Yeah.

Carl Franklin: It must have been those scientists. What do they know?

Pat Hynds: Right.

Richard Campbell: You're reminding me, when you're talking about a group of scientist, that some of the toughest customers I'm out to deal with have been like a company of engineers where they just have a little too much computer skill per user.

Carl Franklin: I was being facetious, by the way. I don't know about you. I love scientists. I am a scientist.

Richard Campbell: It's these very intelligent people who presume that they would know their way around all these stuff that results in deep trouble.

Carl Franklin: That's a problem in general, I think.

Pat Hynds: I think the culture matters. I've been to places where it was a culture of mad scientists.

Richard Campbell: This is on mad.

Pat Hynds: Well, the mad scientist, you know, when I visit customers I usually try to characterize the culture because the culture says a lot about what happens that shouldn't happen behind the scenes like do people take production systems back home to work on. Is somebody liable to take a copy of the back-up to take home with them just because they didn't have enough storage on the server, those kinds of things. Because culture is a big part of security because the real weak point now, as Richard points out, the people are the biggest weak point now.

Carl Franklin: This portion of .NET Rocks! is brought to you by the Haystack Code Generator for .NET, Code Generation on Steroids. Want more control over your Code Gen? You want your code generator to give you Silverlight 4.0, WPF, and ASP.NET CRUD screens? The Haystack Code Generator for .NET will generate entity, data, and business rule classes for all your SQL Server and Oracle tables, views, and stored procedures. Haystack generates ASP.NET, WPF, and Silverlight user controls, View Model classes, and WCF Service Layer classes for true and tier applications. Check out codehaystack.com, download the user manual, and watch the videos from more information on this great product. They host a live webcast every two weeks. You can sign up at pdsa.com/webcast and see how Haystack will shorten your development cycle.

Richard Campbell: Oh, yeah. There's this great SK CD cartoon, Wrench-based Security. It's like I don't care how good your encryption is when I could take a $5 wrench and beat the password out of somebody.

Pat Hynds: Oh, and you've heard about the experiment where there was a company -- so Steve Reilly talks about these things in his session on Social Engineer.

Richard Campbell: Right.

Pat Hynds: I haven't heard him do it in a long while but I really love that session. We're going to try to get him on Locked Down and talk about that soon. But one of the things that -- the famous hacks is people will leave USB keys.

Richard Campbell: Yeah. A guy scattered a bunch of USB keys in a parking lot.

Pat Hynds: Of a bank.

Richard Campbell: Yeah.

Pat Hynds: And three people took it into the building and plugged it into their client machine in the bank and he ran a tracer.

Carl Franklin: Ooh.

Pat Hynds: He had a program that run it and let him know the IP address and all the other information.

Richard Campbell: Which also means that they were setup by default. It auto run the USB key, plugged it in and looked for auto play and run it.

Pat Hynds: Right.

Carl Franklin: That's horrible.

Pat Hynds: That's social engineering though. Because it was not like he walked in the door, went through the duct and was suspended by a wire to do it. He uses peoples' culture and peoples' sense of things to do it.

Richard Campbell: Yeah. And that's not even a tough engineering job, like he didn't actually create incentives around the key. These are just blank keys lying on the ground as opposed to put up a key kiosk with "Get this USB key, you get a great stuff."

Carl Franklin: Right.

Richard Campbell: So you actually create some incentives around it.

Pat Hynds: Yeah.

Carl Franklin: Yeah, no incentive required. The incentive is there's something that might...

Richard Campbell: Ooh, I found something cool.

Carl Franklin: There might be something delicious on this little piece of...

Pat Hynds: Oh, yeah. I love the social engineering thing and unfortunately we don't get to exercise it very often because most of the time when we talk to a client about penetration testing, or a security audit, or in the aftermath of an attack, they don't want to deal with the human factor because they're in denial.

Richard Campbell: Right.

Carl Franklin: Yeah.

Pat Hynds: And the biggest human factor is the internal users. I mean, the most likely person to destroy a company through security breaches is an employee that's been with the company over eight years.

Carl Franklin: An inside job.

Richard Campbell: Really. So not even necessarily a let go employee but a long term employee.

Pat Hynds: Yes. The most likely person to carry out a million dollar, a hack that cost you a million dollars, whether they make a million or not off of it, is an employee, somebody in a position of trust who's been there for at least eight years.

Richard Campbell: And is disgruntled?

Pat Hynds: Yeah or feels that they haven't gotten their due, or is about to launch a competitor, or was passed over for the promotion or the parking spot. They're just too comfortable. They know where the security cameras are and they know where to stand to not be viewed because at one point somebody brought them in and said "Look, look how good the security cameras are. The only place we can't see is in that corner."

Carl Franklin: Pat, somebody is calling you instead of our hot line.

Pat Hynds: Yeah, I know.

Carl Franklin: No, no, no, no. The number is... No, I'm just kidding.

Richard Campbell: Too funny.

Pat Hynds: Yeah.

Carl Franklin: Yeah.

Richard Campbell: All right.

Pat Hynds: Okay, it's off. No, it didn't.

Richard Campbell: No, it didn't. It fooled you.

Pat Hynds: Sorry about that.

Carl Franklin: This is live radio. We can't edit that out.

Richard Campbell: Yeah.

Pat Hynds: I know.

Richard Campbell: It doesn't matter.

Pat Hynds: That's right. So one other thing. I have a conversation free regularly with owners, business owners and I get to a point where most of the time it's, you know, you really should have back-ups. You know, you really should have a disaster recovery plan. Well, this company, the one I'm talking about, the rabidly security focus company, I had an hour meeting with the owner of the company and at that meeting it's usually a very private meeting because we're going to talk about very sensitive security stuff.

Richard Campbell: Sure.

Pat Hynds: In this meeting, I actually got to my ultimate question which is a question that I've only gotten to in a couple of cases because most of the time they can't get to that point because they've got so many small stumbling blocks to deal with.

Richard Campbell: Right.

Pat Hynds: It was, "Look, you have a really great company from a security perspective. We found a couple of things, your staff was horrified by them and they fixed them immediately." So you needed somebody to come in periodically even if you're a rabidly security conscious just to make sure you didn't overlook something. But honestly, there were two big suggestions I had for him and one is if you want to increase physical security, because they had one of those double security doors with sign in. Sorry about the background phone. They had one of those double security doors with sign in and what they ended up doing was they had really good physical security. We told them that they had to add, in order to increase physically security they should add an Armed Response Team with shotguns.

Richard Campbell: Nice.

Carl Franklin: Just briefly, we did have a tweet from Chris Love who suggests the book "The Art of Intrusion" by Kevin D. Mitnick.

Pat Hynds: Oh, Mitnick, yes.

Carl Franklin: On Amazon. Is that a book that you have heard of or read?

Pat Hynds: I've heard of. I haven't read it. Mitnick is the original, pretty much. Captain Crunch is the original hacker from the lore that I've read. He is the guy that found the whistle in a Cap'n Crunch box and figured out that he could unlock long distance phones by playing in the right key.

Richard Campbell: It was the whistle that came in...

Carl Franklin: Was it 2600 hertz or something like that?

Richard Campbell: Something like that, yeah.

Pat Hynds: Yeah.

Richard Campbell: And the whistle that came in a Cap'n Crunch box did best.

Carl Franklin: Right.

Richard Campbell: So you picked up a pay phone, you blew this whistle and you can make free calls.

Carl Franklin: Right.

Pat Hynds: Yeah, yeah. But Mitnick is the first like actual hacker that was chased.

Richard Campbell: And he got caught and then he's like go to jail and worked for the FBI kind of thing. He ended up doing some time and now he's working his white hat, he works on the other side.

Carl Franklin: And he inspired millions of hackers everywhere to commit crimes as a means to get a job.

Richard Campbell: There you go.

Carl Franklin: Yeah. Which, by the way, doesn't really happen anymore.

Pat Hynds: No, no.

Richard Campbell: Okay. I want to get back to the Armed Response Team with shotguns.

Carl Franklin: Right.

Pat Hynds: So I told them, I said "You know, your physical security..." Normally I have to say things like, "You know, you really should have your servers in a room that locks."

Richard Campbell: Nice.

Pat Hynds: And you really should have some security, you should take down the pads of paper with the passwords on them in the server room.

Richard Campbell: Yeah.

Pat Hynds: I'm almost always dealing with this incremental stuff because usually security is so bad. But this company challenged me because they were so good, the best we've ever done security other than the government but I have to say the military...

Richard Campbell: Are in their own league.

Pat Hynds: Because they do have Armed Response Teams.

Richard Campbell: Yes, they really do.

Pat Hynds: And I've been part of them in the past.

Carl Franklin: They scale down the walls.

Pat Hynds: So I've been on Fort Knox, I've been down at Quantico, I've been in a lot of places.

Richard Campbell: So that's what you're doing in a rack, an Armed Response Team. That's a heck of a security breach.

Pat Hynds: Yeah.

Carl Franklin: Put down that USB key.

Pat Hynds: Yeah. The Republican Guards tried to breach our security so I had to go after them.

Carl Franklin: Drop that keyboard.

Pat Hynds: Anyway, so that was one suggestion and they actually considered it. They actually thought about it. The next thing was I had a very sober conversation with the owner. I said, "Look, you know you have a disaster recovery plan and that is to be lauded and you've got this covered and you got this covered and there's one area I haven't seen anything about that most companies have never face," and he was caught by surprise. He's like "That can't be true. We've thought this through completely."

Richard Campbell: We thought of everything.

Pat Hynds: I said "If you plan for if the building is destroyed, you've planned for if the infrastructure is wiped out but you haven't plan as far as I can tell for one to 80% of your staff is dead."

Carl Franklin: Wow.

Richard Campbell: The 9/11 scenario.

Pat Hynds: Yeah. And he said, "Oh." And I said, "You know, you have to either accept that you're out of business or you have to figure out where you're going to get the people at your disaster recovery site that can be trained quickly and know what the training programs are going to be. You're going to make videos and start going through the process of what it would take to do that," and he's like "Yeah. We're out of business." Now it's his decision.

Carl Franklin: Chris Love says there's another book by Mitnick which is The Art of Deception, controlling the human element.

Pat Hynds: Yeah, that's the steps to social engineering sites.

Carl Franklin: Yeah. But I thought it was actually in some ways I could understand if he said either like "Well, we'd want to continue the company for the survivors and the families of those who are gone," or like they did at 9/11 with some of the companies from my understanding, or to say "You know what? If we lose the people, then the company doesn't mean anything." But it was funny because those are the two ultimate questions that I've only been able to ask. I try to work them in for companies that want like the whole view, like "Oh, you really want to know everything that's involve. Okay, here's everything you need to think about and here's the ultimate question." But that was the first time I ever had to confront that with the client. That was very interesting.

Richard Campbell: Yeah. I'm thinking of -- it was Cantor Fitzgerald. It was the company in the World Trade Center that had the top floors of one of the buildings.

Pat Hynds: Yup. And then they can try to continue the company because they – ostensibly. I didn't really follow the story whether they were actually successful and they're still in business, but I know the CEO was on TV quite a bit saying we want to continue this so that we can take care of those who are left behind. That kind of thing.

Richard Campbell: Yeah. There's an interesting point that's part of this. I deal with the same thing when I was doing DR work around -- we were dealing with companies in the Caribbean and being able to tolerate a hurricane and there was a point where it's like there's a point at the level of a hurricane damage where keeping your servers up is just no longer important.

Pat Hynds: Right.

Richard Campbell: Now it's more about getting food.

Pat Hynds: So isn't that also in the scale of your shoes don't matter when you feel like you're going to throw up?

Richard Campbell: Right. Yeah.

Pat Hynds: You'll creep at your shoes later.

Richard Campbell: Yeah. We'll deal with that later.

Carl Franklin: Hey, by the way, we have 22 listeners.

Pat Hynds: Awesome.

Carl Franklin: Yeah.

Richard Campbell: It's like 2002 all over again.

Carl Franklin: Well, you know, this is an odd time for people to be up on a Saturday morning. I'm just saying.

Pat Hynds: Listening to a technical show. No, I appreciate every one of them. Thank you very much.

Carl Franklin: And Michele is coming up next so we got the security 1, 2 punch here.

Pat Hynds: Yeah, you do.

Richard Campbell: Well, we're doing security where it belongs. Right upfront so we're getting north.

Carl Franklin: That's right. Get it out of the way then we can have some fun.

Pat Hynds: If you're not nice, I'll send my Armed Response Team.

Richard Campbell: There you go. So like let's do a little .NET-related security here. Can we talk about the colossal failure that is Code Access security?

Pat Hynds: I knew you're going to say that.

Richard Campbell: Well, why shouldn't we?

Carl Franklin: Why do we even need to talk about it? Doesn't it not exist anymore?

Richard Campbell: Well, yeah. It's hidden in .NET 4.0. It went away, right? First, at least it existed for a couple of versions of .NET and had been ignored and now all of a sudden you don't even ignore it.

Carl Franklin: You can still use it if you want, but nobody is using it. If it's not in, take it out. Did they?

Pat Hynds: No, they didn't take it out. What they did, and I'm simplifying, is they've subsumed it into the framework so that it's there and it's not so onerous for you to do the right thing.

Richard Campbell: Right.

Pat Hynds: And it's not so easy for you to do the wrong thing. The problem with Code Access security was it was the high tech security system that people buy. We spent $5,000 on a security system. We've got motion detectors in every room, and the baby would set it off every time we armed it.

Richard Campbell: Right.

Pat Hynds: So we stopped arming it.

Richard Campbell: Yeah.

Pat Hynds: And then we found that we wanted to put ceiling fans in all the rooms and we found those would set it off and so we didn't arm it. So what happened is what's gotten in the way of Code Access security was living.

Richard Campbell: Yeah. As long as you didn't run any programs, Code Access security works great.

Pat Hynds: It was great, yeah. I like it. I thought it was great. When it first came out, I attended a session by Juval Lowe that was great. He talked about things that I haven't thought about like his stand on Code Access security is, or was back then, that you should remove all the default security and just add what you need.

Richard Campbell: Right.

Pat Hynds: Which was something that I'm a little pissed off occur to me, before he said it.

Carl Franklin: Well, remember, that was before XP Service Pack 2.0.

Pat Hynds: Yes.

Carl Franklin: Which got rid of all those security problems, or fixed all those security problems, and that was also the -- what was it? It was the default in Vista, wasn't it? No, no. In Windows Server. It was the default in Windows Server that everything was locked down by default out of the box. Nothing was enabled. You had to -- what was it? Server 2003 that started that?

Richard Campbell: Yeah. It really got into that.

Pat Hynds: Yeah.

Richard Campbell: The fun stuff was off by default instead of on.

Carl Franklin: Off by default.

Pat Hynds: And then IIS followed suit in 2008, the IIS7.

Carl Franklin: Hey, I've got to give another shout out to Chris Love who sends us another twit. He says eating breakfast, listening to DNR Live, reading blogs, getting a DNR live shout out, priceless.

Pat Hynds: Excellent.

Carl Franklin: A true fan.

Richard Campbell: There you go.

Pat Hynds: That's an awesome weekend. Today is my 22nd wedding anniversary so...

Richard Campbell: What are you doing?

Carl Franklin: Oh, congratulations. Your wife must be really happy about what you're doing right now.

Pat Hynds: She has come to accept that you guys are a part of my life.

Carl Franklin: Oh. Well, give her a big hug for us.

Pat Hynds: I will, I will.

Carl Franklin: Don't forget the flowers.

Pat Hynds: We're going to go up to the White Mountains, take the dogs and go see our favorite covered bridge...

Carl Franklin: That's right. You're in New Hampshire, right?

Pat Hynds: Yeah. I'm working at DDR, the soccer game, and avoid anyone who tries to tell us the score and kill anyone who actually succeeds.

Richard Campbell: Armed Response Team.

Carl Franklin: Oh, by the way, I have ESP. Would you like to know the outcome?

Pat Hynds: US 5. I'm actually a big soccer fan. It's the only sport I watch.

Carl Franklin: Stay away from the psychics.

Pat Hynds: I've been coaching for about 11 years.

Carl Franklin: Oh, really?

Pat Hynds: Yeah. My daughter is going to Dublin. My youngest daughter is going to go to Dublin this fall to study at an American College Dublin, at Trinity college in downtown Dublin, and we're dropping her off and she's going to be playing soccer over there. My oldest is actually in Munich right now and she's probably never going to come home.

Richard Campbell: Munich is a great place.

Pat Hynds: Yeah.

Richard Campbell: It's not surprising that she would fall...

Carl Franklin: Actually in the fall. I'm just saying.

Pat Hynds: Well, she's a senior this year and she said she found her act. She's going to do her masters in London or some place else in like Czech Republic, and now she has found her school in Munich. So I've worked with a friend of mine who gave her an internship over the summer.

Richard Campbell: And you've spent some time in Germany too.

Pat Hynds: Oh, yeah. I've spent a lot of time and we go over every year. My wife is from Germany and I spent three years in the service over there. Well, I guess it was three years because the last six months was interact.

Richard Campbell: Right. And so you've got a family connection really to Germany.

Pat Hynds: Oh, yeah, yeah. We're really tied with it. Every year somebody comes over and spent a couple of weeks during the fall, and we go over every year and spend a week or two and I also have business in Europe as well.

Carl Franklin: Are there any good German restaurants in New Hampshire where you are?

Pat Hynds: There used to be one. It was right on the state line but I think it went away, and then there's a new one that my sister-in-law and my nephews went to that they really liked so I've got to check that one out. But my wife is a great cook as well so I'm big on the German food.

Carl Franklin: My ex-wife's grandfather frequented one of the oldest restaurants in Springfield, Massachusetts called The Fort.

Pat Hynds: Really.

Carl Franklin: And it may be the oldest restaurant in Springfield, Massachusetts.

Pat Hynds: Wow.

Carl Franklin: A German restaurant. When you walk in, there are steins all along a ledge on the ceiling and like the guys got a serious stein collection. Not only that but all sorts of plates, and armor, and swords, and anything that's made of pewter pretty much.

Richard Campbell: It's in this building.

Carl Franklin: Yeah and he's got a -- he died, but he had -- maybe they still do, a security system with laser beams that goes across the ceiling so it always reminded me like a jewel heist when you walk in there. His friends who use to like take their dinner

napkins and toast them up in the air that set off the alarm, you come running out from the kitchen.

Richard Campbell: This is stein defense.

Carl Franklin: Yeah, exactly.

Richard Campbell: Just defending those steins.

Carl Franklin: You know this is the Live Weekend so we can diverge into stuff like this. Great red cabbage and Viennese Schnitzel and...

Pat Hynds: I like Jagerschnitzel.

Carl Franklin: Jagerschnitzel.

Pat Hynds: Jagerschnitzel is a Viennese Schnitzel, a breaded pork cutlet. Pork loin, sirloin cutlet actually. It's got a mushroom sauce, a brown mushroom sauce called Hunter's sauce. Jager, it means hunter.

Richard Campbell: Yeah.

Pat Hynds: So a Jagerschnitzel is a Hunter Schnitzel. They're really good. That's my favorite.

Carl Franklin: So Jagermeister literally means mushroom man?

Richard Campbell: No, it's hunting. The hunt leader.

Carl Franklin: Oh, hunter.

Pat Hynds: Hunting master.

Carl Franklin: Hunting master. Okay.

Pat Hynds: Yeah. Jagermeister. I speak German.

Carl Franklin: Okay. I think Jagermeister is like the nastiest cough syrup kind of crap people like but I can't stand it.

Pat Hynds: So I've been to a couple of places in Germany where the locals come in and their stein is in the beer hall and they take it out of a cubby.

Richard Campbell: They bring it down to fill with beer and use.

Pat Hynds: Exactly, yeah.

Richard Campbell: Storing your own cup at your favorite restaurant. Now you're talking.

Pat Hynds: Yup.

Carl Franklin: That's cool.

Pat Hynds: Yeah. So that's what the guy should have done. It's they bring their own stein and then he can decorate with someone else's stuff.

Carl Franklin: Oh, yeah. You're always thinking.

Richard Campbell: There you go.

Carl Franklin: I must admit, Pat, that I'm a big fan of the Hunter sauce and the pork schnitzel and Schweinshaxe which is a pork knuckle.

Pat Hynds: Yeah.

Carl Franklin: Which sounds nasty but that's where all the really delicious kind of meat is if it's smoked.

Pat Hynds: Have you had wild boar?

Carl Franklin: I know a few wild boars, but no.

Richard Campbell: Nice.

Pat Hynds: So it's actually like, you know, how you've got dark meat in chicken and light meat in chicken?

Carl Franklin: Yeah.

Pat Hynds: Wild boar is like the dark meat pig.

Richard Campbell: It's all dark meat.

Carl Franklin: Whoa.

Pat Hynds: Yeah, it's really good.

Carl Franklin: You ever smoked a wild boar, Richard?

Richard Campbell: I've not smoked a wild boar but I have cooked.

Carl Franklin: Something to put on your list.

Richard Campbell: Yeah. We've done the rotisserie of a boar.

Carl Franklin: Really.

Richard Campbell: Yeah. It's a good way to cook it because you've got to cook it slow, but it's not like the traditional barbeque inside of a smoker. It's on the spit.

Carl Franklin: So you put a wild boar on a spit and turn it over a fire.

Richard Campbell: Yeah. For 12 hours.

Carl Franklin: That's seriously evil.

Pat Hynds: Well, you have done some pig roasts.

Richard Campbell: I have done some pig roasts, yes.

Carl Franklin: So has Carl. That actually was the only pig roast I've ever eaten.

Richard Campbell: That was his birthday, yeah.

Pat Hynds: I know, yeah.

Carl Franklin: On my 40th birthday, we had a pig. Not on a spit though.

Richard Campbell: No.

Carl Franklin: It was smoked.

Richard Campbell: It was done nicely.

Pat Hynds: Ah, okay. It was good. So Michele is your next guest. That's interesting. I saw you've got Charles Petzold. You've got a very interesting cast of characters.

Carl Franklin: Yeah, it should be a good weekend. Like I say it's not all going to be business. We just sort of want to shoot the breeze. The real idea of the Live Weekend is to get people out there listening to talk back to us. I mean, all of our guests have been on the show before and some recently, so it's a good opportunity if people have questions about some of the stuff that we've been talking about on .NET Rocks! for them to call in and ask.

Pat Hynds: Oh, yeah. I think that's great. Is there a way to podcast stream it so if you, you know? Is there a podcast subscription or you've got to be on the internet and live stream it?

Carl Franklin: For this weekend, you have to listen live. But we are recording the shows and they will become Thursday shows for the next 35 weeks.

Pat Hynds: Wow.

Carl Franklin: Yeah.

Pat Hynds: That's excellent.

Richard Campbell: Yeah, we are racking and stacking the content this weekend.

Pat Hynds: Nice. Very nice.

Richard Campbell: Yeah. It's going to change up the dynamic a little bit.

Pat Hynds: Cool. You have another one in the plan maybe or is this a one off?

Carl Franklin: Well, we don't know. We're going to see how well received it is and how people like the shows the second time around on .NET Rocks!

Pat Hynds: I'd say 22 listeners at this time of the morning on a Saturday is pretty damned successful.

Carl Franklin: Yeah, I think so.

Pat Hynds: Is your grandmother tuned in because that's who I thought was the only one.

Carl Franklin: We have a tweet from JRCS3. I like Texas Schnitzel. Are you going to talk food as the stack question? What's your favorite deep fried food? Mars bars, dude. No, I've...

Pat Hynds: Never tried that.

Carl Franklin: Deep-fried candy bar. I don't know.

Pat Hynds: I really want to try one of those though.

Carl Franklin: I'll tell you what. So Hanafin'sPub is right downstairs from us and this is the sort of the studio hangout. It's like my den, you know. Anyway, they just moved to a new location right next door. They moved one door over and they built the bar that looks almost exactly the same as the old one.

Pat Hynds: That's cool.

Carl Franklin: So people walk in and the do a double take and they're like "Doesn't, this door..."

Richard Campbell: Would you..? Can anybody...?

Carl Franklin: Where's t h e ...? What happened to the...? You know, it's great. I love watching people come up to the door outside. I'm sitting out on the porch and I'm just looking at them getting confused. Anyway, they have a deep frier and my band is actually, Solvo, my band who you're going to hear on Monday, we're going to be playing there

every Thursday night doing this New Orleans night. So I got to sit down with the chefs, or the chef, and talk about the food that they're going to serve because it's New Orleans food. One of the things they're going to do is Deep Fried Shrimp Po' Boys.

Richard Campbell: Nice.

Carl Franklin: Yeah.

Pat Hynds: Oh.

Carl Franklin: So they had never done that before. So I went to the grocery store and I got some great ingredients and they let me like cook up some Po' Boys.

Pat Hynds: Well, Po' Boy is a sub or a hero.

Carl Franklin: That's right. A Po' Boy is a grinder which we call them here in New London, in New England, or submarine sandwich or hero or hoagy or whatever you want to call them, but you basically take the bread and you grill it on the grill with butter so it gets crispy and brown when you do that on a really hot grill and so the bread is soft but the face of it is really crispy, and then you get deep fried shrimp which are in a sort of a cajin butter.

Richard Campbell: A little spicy.

Carl Franklin: A little spicy and lettuce, tomato, and mayonnaise and some people put like a remoulade sauce which is sort of if you could think of sort of a little horseradishy chilly cayenne little cage in spice mayonnaise-based little ketchup, that kind of stuff, remoulade, put it on the...

Richard Campbell: I was just in New Orleans eating Po' Boys.

Carl Franklin: Yeah.

Pat Hynds: I think I have to go eat breakfast. So my favorite deep-fried food would have to be scallops.

Carl Franklin: Really.

Richard Campbell: Deep-fried scallops?

Pat Hynds: I love fried scallops. I don't eat them very often, but it's my favorite deep-fried food because they just -- it's something about the combination of frying a scallop that makes it really great.

Carl Franklin: Yeah. Scallops are great. Now, do you like bay scallops or sea scallops? Because the bay scallops are the little ones, and the sea scallops are the big ones.

Pat Hynds: I usually eat the sea scallops as on tray, but the bay scallops as a side.

Carl Franklin: Yeah.

Richard Campbell: There you go.

Pat Hynds: Yeah.

Carl Franklin: All right.

Richard Campbell: We didn't talk a lot of security today.

Carl Franklin: Well, no, we did a little.

Pat Hynds: We did. We got a lot of...

Carl Franklin: So in five minutes or less, as a developer and let's say that you're using, I don't know, Team Foundation System or TFS, and you're using Team System tools in Visual Studio, is there anything in particular that you need to be worried about as a developer that falls outside the realm of development IT?

Pat Hynds: Yes. I find, as we start doing the Locked Down shows on security, that I keep saying the same thing and I'm trying not to say it without sounding like a broken record. I've discovered that the most important thing is the Threat Model and it's something that almost no one does. That is if you don't have a Threat Model, if you don't know what you're worried about, like everyone knows what they're physically worried about. I'm worried about driving over a bridge and not being able to get the family out of the car. I'm worried about spiders eating in the night. Whatever you're afraid of, you know that personally. Developers have to develop the same kind of well developed threat model in their mind relative to their systems. Companies need to do it more exactly based on a project basis because otherwise you're at the whims of all the fear, uncertainty, and doubt that everybody is broadcasting.

Carl Franklin: Yeah.

Pat Hynds: My brother is in the security space and we're trying very hard and I think we're going to be heroically successful of not bringing in any fear mongers on the show because there are a lot of people out there who just want to wave the banner of this is going to get you killed.

Carl Franklin: Right.

Pat Hynds: It's the same thing the news does, it's "Your lettuce maybe killing you. Details at 11."

Carl Franklin: Yeah, that's right. They have a product or a service to sell and the way they do that is by...

Richard Campbell: Making you afraid.

Carl Franklin: Scaring you into buying it. Yeah.

Pat Hynds: Right. Now that's not to say that letting someone know what a vulnerability could be is, but it's almost always over hyped.

Carl Franklin: Right. You have to put it in proper perspective.

Pat Hynds: Right. Which is unpopular for the sales person. But if you understand, if you have a well-developed thread model, then you understand it gives you a spam filter on that stuff. You know what? That doesn't matter to me because it's not part of my threat model because my threat model lies in this area.

Carl Franklin: Yeah.

Pat Hynds: I'm more worried about social issues, not that encryption issue because I've already manage that in my threat model in this way, and what I found is most applications don't have one. It's something you can develop most of the time, 90% of the way before the application is even developed because you understand how it's going to be deployed, you understand how it's going to be used, you understand where it's going to be deployed. Even if you don't know where the buttons are going to be, you can come up with a very good threat model for an application or for a system and then you can apply that as a spam filter to all the security issues that come up.

Carl Franklin: Okay. Pat, it's been a pleasure having you as the first guest on our Live Weekend and very appropriately so.

Pat Hynds: Woohoo.

Carl Franklin: We're going to take about a 10-minute break and we'll be back at about 9:05 with Michele Leroux Bustamante. So Pat, thank you very much.

Pat Hynds: Thanks for having me. I'll talk to you guys soon.

Carl Franklin: All right. And before we go, shout out to Ger O'Donnell, I'm not sure if it's a hard or soft G, who says by email not just all breakfast listeners. We're listening here in sunny Cork, Ireland. You're sounding good, guys.

Pat Hynds: Awesome.

Carl Franklin: All right. We'll be back.

[Music]

Carl Franklin: .NET Rocks! is recorded and produced by PWOP Productions, providing professional audio, audio mastering, video, post production, and podcasting services, online at www.pwop.com. .NET Rocks! is a production of Franklins.NET, training developers to work smarter and offering custom onsite classes in Microsoft development technology with expert developers, online at www.franklins.net. For more .NET Rocks! episodes and to subscribe to the podcast feeds, go to our website at www.dotnetrocks.com.